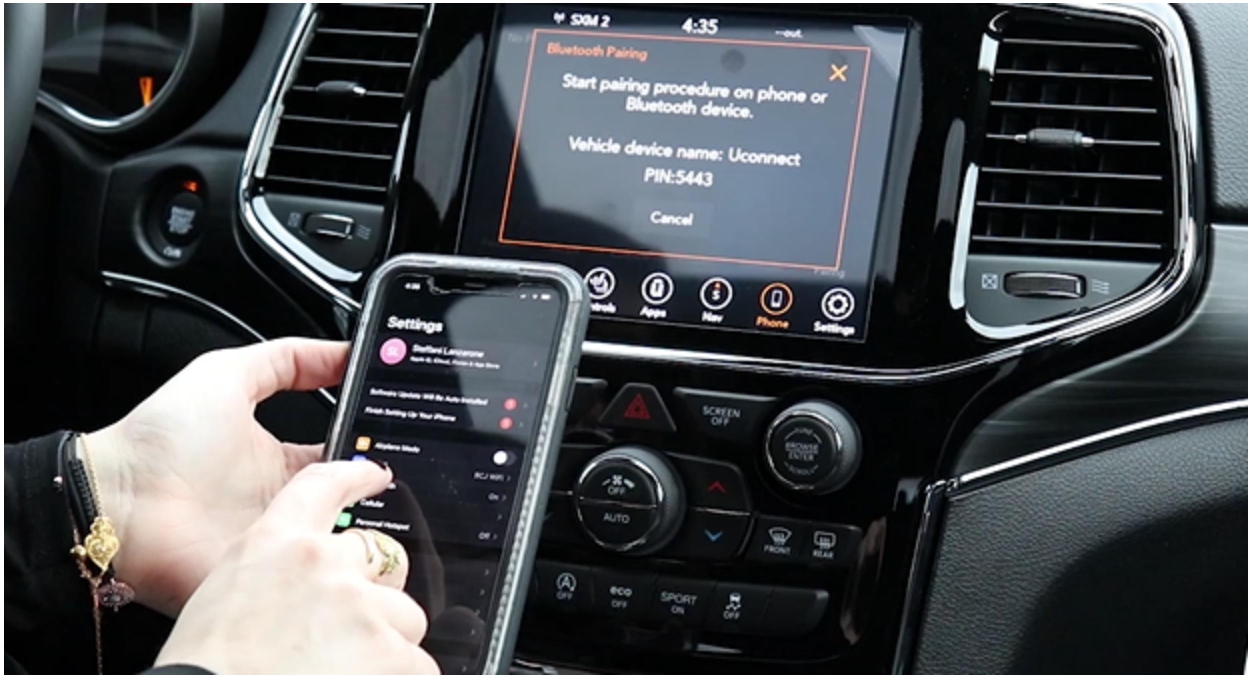
EXHIBIT 7

US Patent 6,928,166 Versus Chrysler Uconnect (3 and 4)



Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

1. An authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising:

means for acquiring an external factor which is associated with a security level;

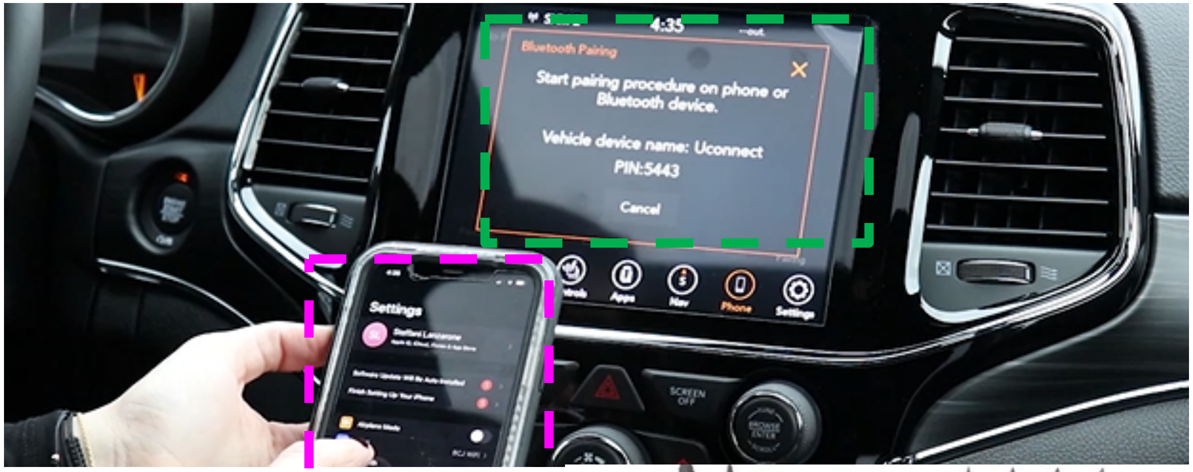
means for selecting a security level from a plurality of security levels in accordance with the external factor;

means for receiving a request for an authentication and authentication information from the device;

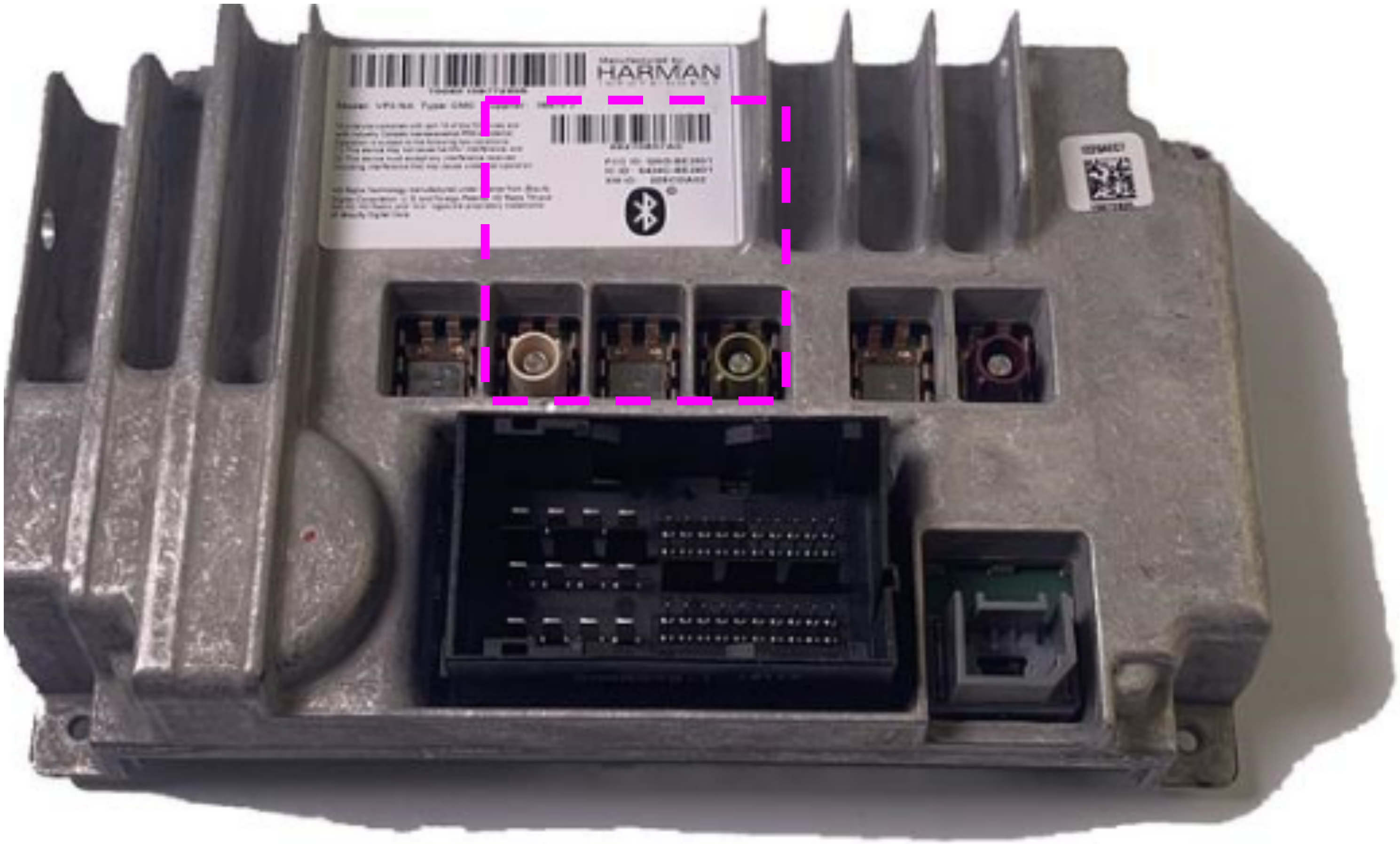
means for checking whether the received information from the device is valid or not depending on the selected security level; and

means for sending a response of the check result which authenticates or rejects the device thereto.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

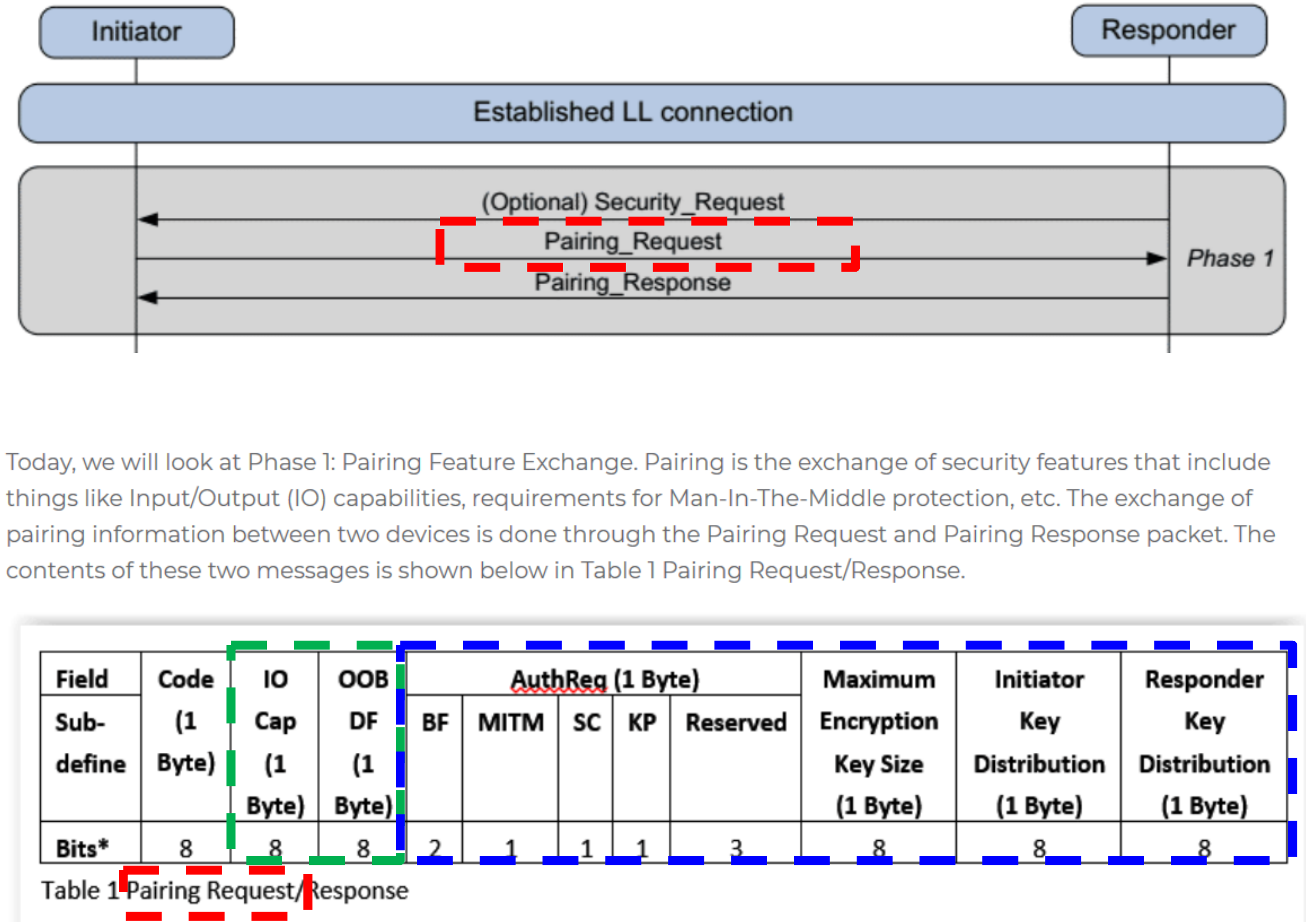
Claim 1	
1. An authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising:	Source: https://www.brownsjeepchryslerdodge.com/how-to-pair-your-phone-to-uconnect/ "How-To Pair Your Phone to UConnect"  4:35 Bluetooth Pairing Start pairing procedure on phone or Bluetooth device. Vehicle device name: Uconnect PIN:5443 Cancel Apps Nav Phone Settings Settings SCREEN OFF BROWSE ENTER https://www.factoryradioparts.com/products/2013-2014-2015-2016-2017-2018-uconnect-with-8-4inch-touch-screen-vp4-ra4-na-radio https://www.factoryradioparts.com/products/2013-2014-2015-2016-jeep-grand-cherokee-summit-trailhawk-srt-latitude-ram-1500-2500-3500-4500-5500-uconnect-8-4a-vp3-ra3-na-radio-infotainment-module

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

Claim 1	
means for acquiring an external factor which is associated with a security level;	

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

Claim 1	
means for acquiring an external factor which is associated with a security level;	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/



Today, we will look at Phase 1: Pairing Feature Exchange. Pairing is the exchange of security features that include things like Input/Output (IO) capabilities, requirements for Man-In-The-Middle protection, etc. The exchange of pairing information between two devices is done through the Pairing Request and Pairing Response packet. The contents of these two messages is shown below in Table 1 Pairing Request/Response.

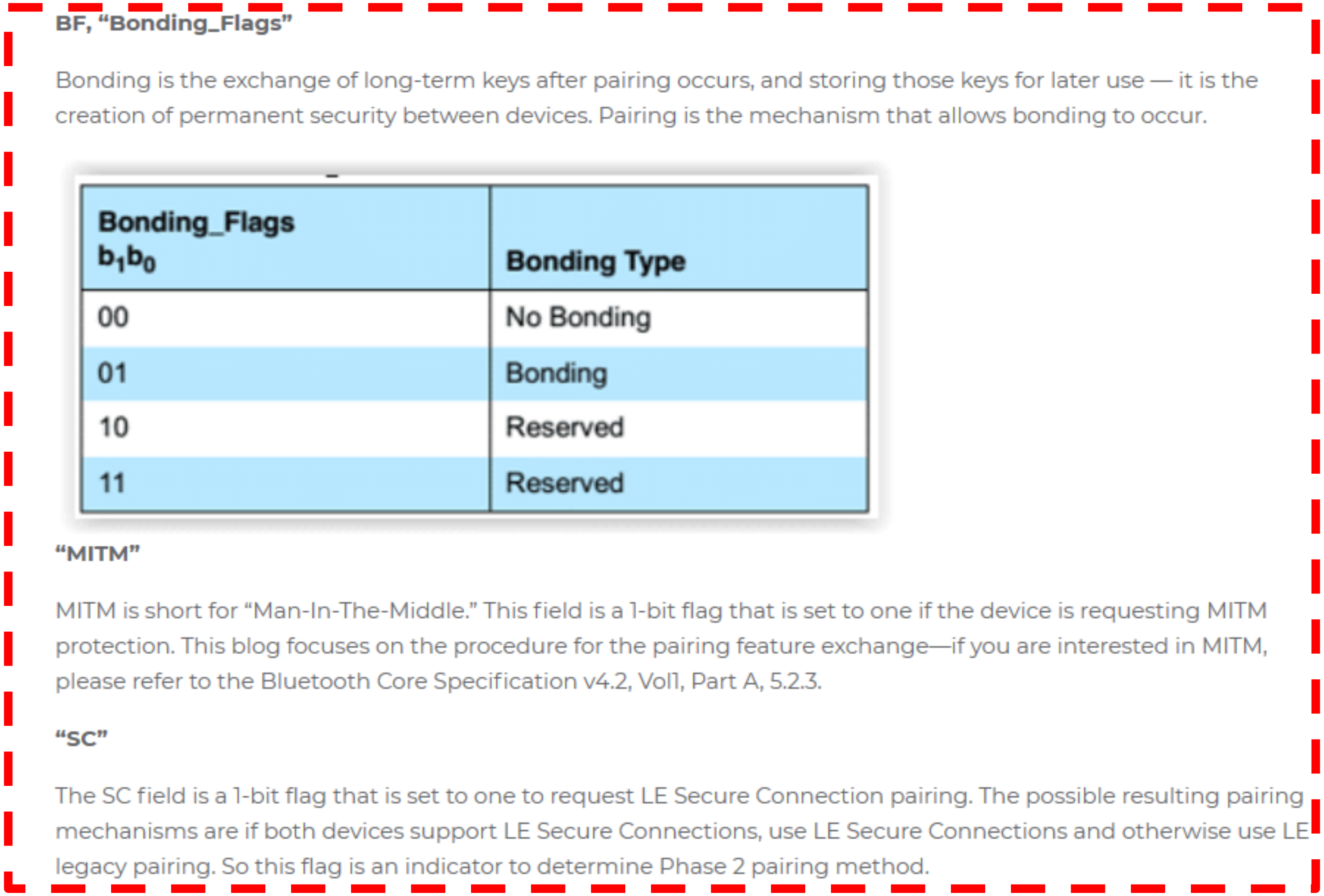
Field Sub-define	Code (1 Byte)	IO Cap (1 Byte)	OOB DF (1 Byte)	AuthReq (1 Byte)					Maximum Encryption Key Size (1 Byte)	Initiator Key Distribution (1 Byte)	Responder Key Distribution (1 Byte)
				BF	MITM	SC	KP	Reserved			
Bits*	8	8	8	2	1	1	1	3	8	8	8

Table 1 Pairing Request/Response

Claim 1

means for selecting a security level from a plurality of security levels in accordance with the external factor;

Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/



BF, "Bonding_Flags"

Bonding is the exchange of long-term keys after pairing occurs, and storing those keys for later use — it is the creation of permanent security between devices. Pairing is the mechanism that allows bonding to occur.

Bonding_Flags **b_1b_0**	**Bonding Type**
00	No Bonding
01	Bonding
10	Reserved
11	Reserved

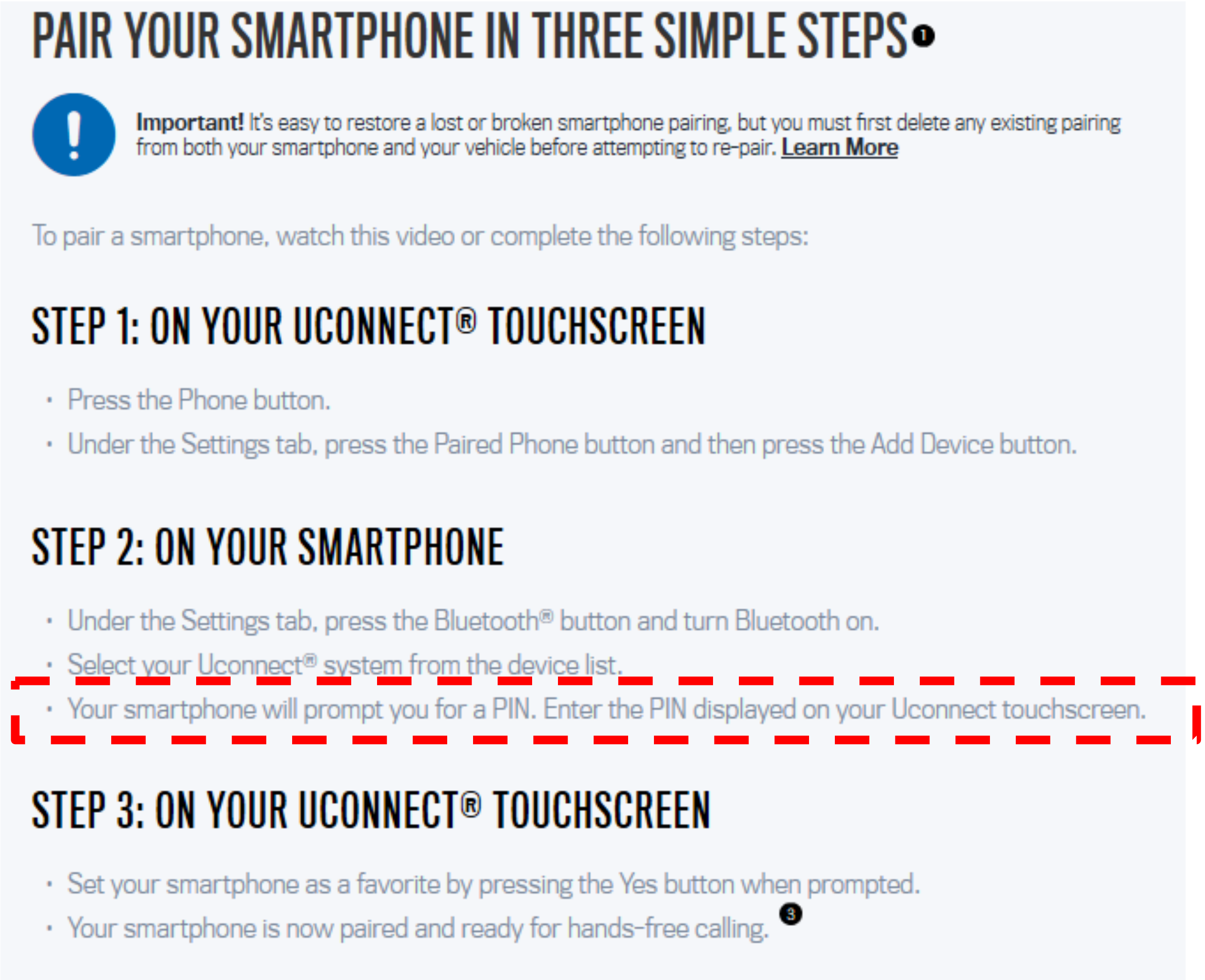
"MITM"

MITM is short for "Man-In-The-Middle." This field is a 1-bit flag that is set to one if the device is requesting MITM protection. This blog focuses on the procedure for the pairing feature exchange—if you are interested in MITM, please refer to the Bluetooth Core Specification v4.2, Vol1, Part A, 5.2.3.

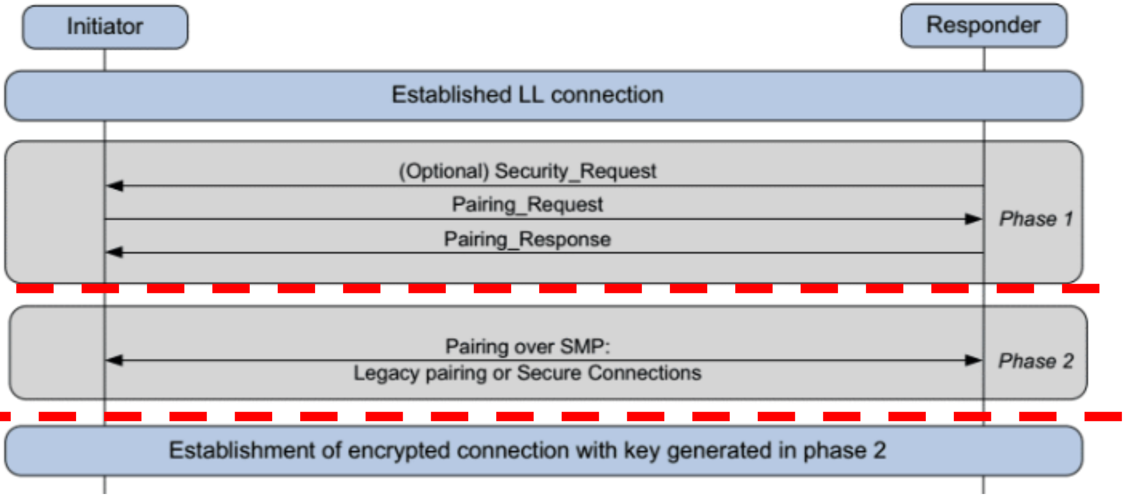
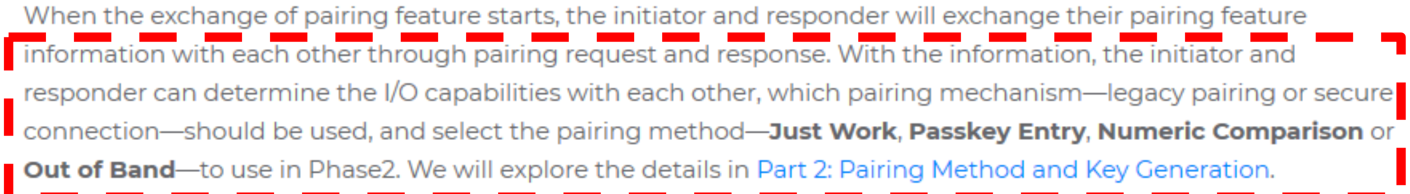
"SC"

The SC field is a 1-bit flag that is set to one to request LE Secure Connection pairing. The possible resulting pairing mechanisms are if both devices support LE Secure Connections, use LE Secure Connections and otherwise use LE legacy pairing. So this flag is an indicator to determine Phase 2 pairing method.

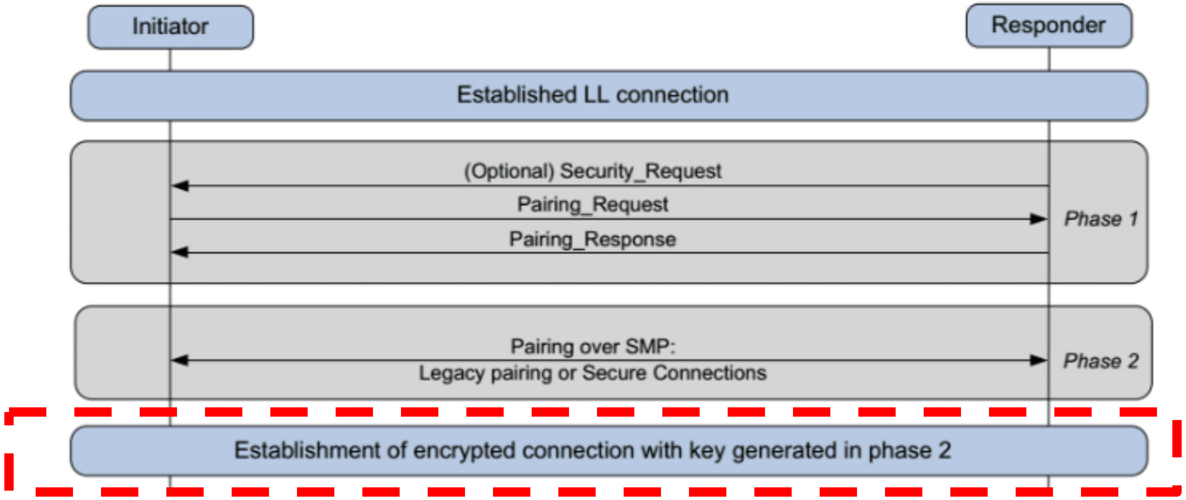
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

Claim 1	
means for receiving a request for an authentication and authentication information from the device;	Source: https://www.mopar.com/en-us/technology/bluetooth-pairing.html  PAIR YOUR SMARTPHONE IN THREE SIMPLE STEPS ❶ **Important!** It's easy to restore a lost or broken smartphone pairing, but you must first delete any existing pairing from both your smartphone and your vehicle before attempting to re-pair. **Learn More** To pair a smartphone, watch this video or complete the following steps: STEP 1: ON YOUR UCONNECT® TOUCHSCREEN - Press the Phone button. - Under the Settings tab, press the Paired Phone button and then press the Add Device button. STEP 2: ON YOUR SMARTPHONE - Under the Settings tab, press the Bluetooth® button and turn Bluetooth on. - Select your Uconnect® system from the device list. - Your smartphone will prompt you for a PIN. Enter the PIN displayed on your Uconnect touchscreen. STEP 3: ON YOUR UCONNECT® TOUCHSCREEN - Set your smartphone as a favorite by pressing the Yes button when prompted. - Your smartphone is now paired and ready for hands-free calling. ❸

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

Claim 1	
means for checking whether the received information from the device is valid or not depending on the selected security level; and	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/  Initiator Responder Established LL connection (Optional) Security_Request Pairing_Request Pairing_Response Phase 1 Pairing over SMP: Legacy pairing or Secure Connections Phase 2 Establishment of encrypted connection with key generated in phase 2  When the exchange of pairing feature starts, the initiator and responder will exchange their pairing feature information with each other through pairing request and response. With the information, the initiator and responder can determine the I/O capabilities with each other, which pairing mechanism—legacy pairing or secure connection—should be used, and select the pairing method—**Just Work**, **Passkey Entry**, **Numeric Comparison** or **Out of Band**—to use in Phase2. We will explore the details in Part 2: Pairing Method and Key Generation.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Uconnect

Claim 1	
means for sending a response of the check result which authenticates or rejects the device thereto.	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/  Initiator Responder Established LL connection (Optional) Security_Request Pairing_Request Pairing_Response Phase 1 Pairing over SMP: Legacy pairing or Secure Connections Phase 2 Establishment of encrypted connection with key generated in phase 2